UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/691,170	10/22/2003	Brant L. Candelore	80398P558D	6531

8791 7590 09/27/2007

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
LASHLEY, LAUREL L	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
09/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

MN

Office Action Summary	**Application No.** 10/691,170	**Applicant(s)** CANDELORE, BRANT L.	
	Examiner Laurel Lashley	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8 and 23-25,27,32-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,23-25,27,32-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's amendments with respect to claims 1, 4 – 5, 23, 27, 32 and new claims 33 – 34 filed 07/16/07 have been accepted. Applicant's amendments to the claims however have introduced anew claim objection.

Claim Objections

2. Claim 27 is objected to because it depends from canceled claim 26. When a claim has been canceled, the remaining dependent claims must also be canceled or amended to depend from pending claims. Claim 27 has been treated on the merits that it depends from independent claim 23, however Applicant is requested make necessary corrections to the claim.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 07/18/07 was filed before any final Office Action. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Response to Arguments

4. Applicant's arguments filed 07/16/07 have been fully considered but they are not persuasive. It is Applicant's assertion that Pinder does not teach a first process block to decrypt a message using the unique key to produce a key, where the key is formed using a mating key generator. The Examiner respectfully disagrees. Pinder discloses the process of a mating key generator where a key is encrypted then using this key and a second key to decrypt thereby recovering an encrypted second key in plain format (i.e.: "E_{kpr}(MSK)", "E_{msk}(CW)", and "E_{cw}(Service)") (see Figure 2B and associated text in col. 7: lines 4 – 16). Ferraro discloses the particulars of the mating key generator (see col. 1: Lines 16-23). As such the combination discloses the limitations of Applicant's claimed invention.

Moreover, Applicant contends that Zhang does not disclose the descrambler IC with the second process being a finite state machine. The Examiner observes that the Applicant's argument is against the references individually, and thus one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Taken in view of Pinder which discloses a descrambler IC, Zhang's disclosure of hardware which includes a processor implemented as a finite state machine specific to an IC (see col. 5: lines 55 – 60) the combination discloses Applicant's claim limitation.

Furthermore, Applicant's arguments with respect to claims 1 – 8, 23 – 25, 27, and 32 – 34 are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1 – 2 and 4 – 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pinder et al. (US Pat. No. 6424717), hereafter "Pinder" further in of view of Ferraro (US Pat. No. 5151782), hereafter "Ferraro".

> Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

6. With regard to claim 1, Pinder discloses a descrambler integrated circuit (IC) adapted to receive scrambled digital content, a message and an encrypted descrambling key (Fig. 2B), comprising:

a local memory to store a unique key (Fig. 2B: items 232 and Kpr);

a first process block to decrypt a message using the unique key to produce a key, (Fig. 2B, Items: 234, E_{kpr}(MSK), Kpr, and MSK indicate process block to decrypt a message using unique key to produce a key respectively)

a second process block using the key to decrypt the encrypted descrambling key and to recover a descrambling key; (Fig. 2B: item 236, MSK, E_{msk}(CW), CW indicate second process block using the key to decrypt the encrypted descrambling key and to recover the descrambling key respectively) and

a descrambler using the descrambling key to descramble the scrambled digital content and to produce digital content in a clear format (Fig. 2B: item 238, CW, E_{cw}(service), Service indicate a descrambler using the descrambling key to descrambler the scrambled digital content to produce digital content in a clear format respectively), *but Pinder does not disclose* the key being formed from a mating key generator that comprises an identifier of a supplier of the scrambled digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider.

On the other hand, Ferraro discloses a message comprises an identifier of a supplier of the scrambled digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider (col. 1: Lines 16-23, "HBO" indicates identifier of a supplier of the scrambled digital content).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Pinder to include an identifier of a supplier of the scrambled digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider, as taught by Ferraro to provide more flexible and versatile for switching equipment in the head-end of each cable system of a network of such system (col. 3: lines 4-6).

7. With regard to claim 2, Pinder discloses the descrambler IC (Fig. 2B), wherein the unique key is loaded into the local memory during manufacture of the descrambler IC (col. 11: lines 51-33).

8. With regard to claim 7 and similar claim 34, Pinder discloses the descrambler IC (Fig. 2B) wherein the first process block and the second process block are logic operating in accordance with one of the following: Data Encryption Standard (DES, Advanced Encryption Standard (AES), and Triple DES (Fig. 3: item 339 and 343).

Claims 3 and 32 is rejected under 35 USC 103(a) as unpatentable over Pinder and Ferraro in view of Zhang et al (US Pat. No. 6550008), hereafter "Zhang".

9. With regard to claim 3, Pinder discloses the descrambler IC (Fig. 2B) with the second process block (Fig. 2B: Item 236). However, Pinder does not disclose the descrambler IC, wherein the second process block is a finite state machine.

However, Zhang discloses the descrambler IC, wherein the second process block is a finite state machine (col. 5: lines 55-60).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Pinder to include the second process block is a finite state machine, as taught by Zhang to improve protection scheme for broadcast signals or other transmitted information (col. 1: lines 40-43).

10. With regard to claim 32, Pinder's reference has already been discussed. However, Pinder does not discloses a first process block controlled by a non-CPU based state machine to decrypt a message using the unique key to produce a key; a second process block controlled by a non-CPU based state machine using the key to decrypt the encrypted descrambling key and to recover a descrambling key.

However, Zhang discloses a first process block controlled by a non-CPU based state machine (col. 5: lines 57-59) to decrypt a message using the unique key to produce a key; a second process block controlled by a non-CPU based state machine (col. 5: lines 57-59) using the key to decrypt the encrypted descrambling key and to recover a descrambling key *but does not expressly disclose* the message is a mating key generator that comprises an identifier of one or more of (i) a manufacturer of a digital device employed with the descrambler IC, (ii) a service provider identifier, and (iii) a conditional access (CA) provider identifier.

However Ferraro discloses the message is a mating key generator that comprises an identifier of one or more of (i) a manufacturer of a digital device employed with the descrambler IC, (ii) a service provider identifier, and (iii) a conditional access (CA) provider identifier (col. 1: Lines 16-23, "HBO" indicates identifier of a supplier of the scrambled digital content).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Pinder to include a first process block controlled by a non-CPU based state machine to decrypt a message using the unique key to produce a key, and a second process block controlled by a non-CPU based state machine (col. 5: lines 57-59) using the key to decrypt the encrypted descrambling key and to recover a descrambling key, as taught by Zhang to improve protection scheme for broadcast signals or other transmitted information (col. 1: lines 40-43) and to incorporate that the message is a mating key generator that comprises an identifier of one or more of (i) a manufacturer of a digital device employed with the descrambler IC, (ii) a service provider identifier, and (iii) a conditional access (CA) provider identifier as taught by Ferraro to provide more flexible and versatile for switching equipment in the head-end of each cable system of a network of such system (col. 3: lines 4-6).

11. With regard to claim 5, Pinder discloses the descrambler IC (Fig. 2B), with the mating key generator (Fig. 2B: item "E_{kpr}(MSK)", "E_{msk}(CW)", and "E_{cw}(Service)", indicate mating key generator(s)) that enables transmission of the scrambled digital content and the mating key generator message to the descrambler IC (Fig. 3: Item 331, "Transmission Medium", Item 329 "encrypted content", Item 315 "EMM", and Item 333, "Service Reception".

However Pinder does not disclose the descrambler, wherein the mating key generator further comprises an identifier that identifies a provider of a system that enables transmission of the scrambled digital content and the mating key generator message to the descrambler IC.

On the other hand, Ferraro discloses a message further comprises an identifier that identifies a provider of a system that enables transmission of the scrambled digital content and the mating key generator message to the descrambler IC (col. 2: lines 19-22, "an individual cable operator" indicates identifier that identifies a provider of a system that enables transmission of the scrambled digital content and the mating key generator message to the descrambler IC, respectively).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Pinder to include an identifier of a supplier of the scrambled digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider, as taught by

Ferraro to provide more flexible and versatile for switching equipment in the head-end of each cable system of a network of such system (col. 3: lines 4-6).

12. With regard to claim 6, Pinder discloses the descrambler IC (Fig. 2B), with the mating key generator (Fig. 2B: item "E_{kpr}(MSK)", "E_{msk}(CW)", and "E_{cw}(Service)", indicate mating key generator(s)), and a conditional access (CA) system which the scrambled digital content is transmitted (Fig. 1: item 101) and a mating key sequence number (col. 6: lines 25-29).

However, Pinder does not disclose the mating key generator further comprises (i) an identifier that identifies a conditional access (CA) system provider over which the scrambled digital content is transmitted

On the other hand, Ferraro discloses the mating key generator further comprises (i) an identifier that identifies a conditional access (CA) system provider over which the scrambled digital content is transmitted (col. 5: lines 33-35, "Video Cipher II" indicates an identifier that identifies a conditional access (CA) system provider over which the scrambled digital content is transmitted).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Pinder to include an identifier of a supplier of the scrambled digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider, as taught by Ferraro to provide more flexible and versatile for switching equipment in the head-end of each cable system of a network of such system (col. 3: lines 4-6).

Claim 8 and similar claim 33 is rejected under 35 USC 103(a) as unpatentable over Pinder and Ferraro further in view of Alve et al (US Pat. No. 6959090), hereafter "Alve".

13. With regard to claim 8 and similar claim 33, Pinder disclose the descrambler IC (Fig. 2B) with the unique key (Fig. 2B: items 232 and Kpr). However, Pinder does not disclose the unique key is a one-time programmable value that cannot be read or overwritten once programmed.

Alve, on the other hand, discloses a one-time programmable value that cannot be read or overwritten once programmed (Fig. 4: item 203 and 204).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Pinder to include such that the unique key is a one-time programmable value that cannot be read or overwritten once programmed, as taught by Alve to protect recorded content from illicit reproduction and distribution (col. 1, lines 27-28).

Claims 23 – 25 and 27 are rejected under 35 USC 103(a) as unpatentable over Pinder and Ferraro in view of Alve, and father in view of Kocher et al. (US Pat. No. 6640305), hereafter "Kocher".

14. With regard to claim 23, Pinder discloses a descrambler integrated circuit adapted to receive scrambled digital content and to descramble the scrambled digital content (Fig. 2B), comprising:

a first process block to decrypt a message using a unique key to produce a first key (Fig. 2B, Items: 234, E_{kpr}(MSK), Kpr, and MSK indicate process block to decrypt a message using unique key to produce a key respectively);

a second process block to receive an encrypted second key and, using the first key, to decrypt the encrypted second key in order to recover the second key in a non-encrypted format (Fig. 2B: item 236, MSK, E_{msk}(CW), CW indicate second process block using the key to decrypt the encrypted descrambling key and to recover the descrambling key in a non-encrypted format respectively); and

a descrambler using the second key in the non-encrypted format to descramble the scrambled digital content and to produce digital content in a clear format (Fig. 2B: item 238, CW, E_{cw}(service), CW and Service indicate a descrambler using the descrambling key in the non-encrypted format to descrambler the scrambled digital content to produce digital content in a clear format respectively).

However, Pinder does not disclose the unique key is a one-time programmable value that cannot be read or overwritten once programmed.

Alve, on the other hand, discloses a one-time programmable value that cannot be read or overwritten once programmed (Fig. 4: item 203 and 204) *but does not expressly disclose* the message is a mating key generator that comprises an identifier of one or more of (i) a manufacturer of a digital device employed with the descrambler IC, (ii) a service provider identifier, and (iii) a conditional access (CA) provider identifier.

However Ferraro discloses the message is a mating key generator that comprises an identifier of one or more of (i) a manufacturer of a digital device employed with the descrambler IC, (ii) a service provider identifier, and (iii) a conditional access (CA) provider identifier (col. 1: Lines 16-23, "HBO" indicates identifier of a supplier of the scrambled digital content).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Pinder to include such that the unique key is a one-time programmable value that cannot be read or overwritten once programmed, as taught by Alve to protect recorded content from illicit reproduction and distribution (col. 1, lines 27-28) and to incorporate disclose the message is a mating key generator that comprises an identifier of one or more of (i) a manufacturer of a digital device employed with the descrambler

IC, (ii) a service provider identifier, and (iii) a conditional access (CA) provider identifier as taught by Ferraro to provide more flexible and versatile for switching equipment in the head-end of each cable system of a network of such system (col. 3: lines 4-6).

Furthermore, neither Pinder nor Alve discloses a first process block to encrypt a message using a unique, one-time programmable key to produce a first key;

Kocher, on the other hand discloses a first process block (Fig. 11: item 1130) to encrypt (Fig. 11: Item "Pseudo-asymmetric transform" and 1140) a message using a unique one-time programmable key to produce a first key.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify methods of Pinder and Alve to include such that the first process block to encrypt a message using a unique, one-time programmable key to produce a first key, as taught by Kocher to distribute content decryption keys in encrypted form to a tamper-resistant cryptographic unit to prevent any attacks (col. 2: lines 45-51).

15. With regard to claim 24, Pinder discloses the descrambler IC (Fig. 2B), wherein the encrypted second key is an encrypted service key (Fig. 2B: item "E_{msk}(CW)" indicates encrypted service key) associated with at least one selected tier of service (Fig. 22: item 2229, col. 36: lines 56-57, IPPV or NVOD indicates tier of service).

16. With regard to claim 25, Pinder discloses the descrambler IC (Fig. 2B) with the encrypted second key is an encrypted descrambling key (Fig. 2B: item "E_{msk}(CW)" indicates encrypted service key is an encrypted descrambling key).

However, neither Pinder nor Alve discloses the encrypted second key is an encrypted descrambling key from a smart card in communication with the descrambler IC.

Kocher, on the other hand, discloses the encrypted second key is an encrypted descrambling key from a smart card in communication with the descrambler IC (col. 21: lines 47-49).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify methods of Pinder and Alve to include such that the encrypted second key is an encrypted descrambling key from a smart card in communication with the descrambler IC, as taught by Kocher to distribute content decryption keys in encrypted form to a tamper-resistant cryptographic unit to prevent any attacks (col. 2: lines 45-51).

17. With regard to claim 27, Pinder discloses the descrambler IC (Fig. 2B) wherein the mating key generator (Fig. 2B: Item MSK indicates a mating key generator) encrypted by the first process block further using the unique key to produce a result being the first key (Fig. 2B, Items: 234, E_{kpr}(MSK), Kpr, and MSK indicate process block to decrypt a message using unique key to produce a key respectively)

Conclusion

18. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Laurel Lashley whose telephone number is 571-272-0693. The examiner can normally be reached on Monday - Thursday, alt Fridays btw 7:30 am & 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Laurel Lashley
Examiner
Art Unit 2132
19 September 2007

GILBERTO BARRUN JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100